NetApp

eBook

Worldwide Data Privacy Regulations Compared

Executive Summary

Data has become a fungible asset for nearly every organization, no matter if they are profit, non-profit, large, or small. The combination of increased technological resources for data collection and the rise of inexpensive and potentially limitless cloud storage, organizations store massive amounts of data on private individuals and in many cases use this data as a source of revenue.

From the standpoint of the individuals whose personal information is being bought and sold, that is a problem. The EU made a groundbreaking shift to address these concerns by introducing the General Data Protection Regulation, or GDPR. This data privacy regulation protects the data privacy of EU citizens and residents no matter where in the world the company using that data is located.

Since then, similar legislation has been enacted in nations around the world, including the California Consumer Privacy Act (CCPA) in the United States, the Lei Geral de Proteção de Dados Pessoais (LGPD) in Brazil, and Protection of Personal Information Act (POPIA) in South Africa.

Which of these laws is your organization going to be affected by and what kind of differences are there between them? In this ebook we will give you an easy way to compare these data privacy regulations from around the world so that you can better plan for how you will meet your company's unique data privacy requirements.

Comparison Table: Worldwide Data Privacy Regulations

	GDPR	CCPA	LGPD	POPI
Territorial Scope	Global	Statewide and global	Global	Restricted to organizations that are either based or process personal data in South Africa
Mandatory DSAR response times	Generally within a month	45-day window, with extensions of up to 90 days permitted.	Within 15 days	Within a reasonable time period
DPO	Mandatory for public-sector bodies and companies that process personal data at scale	None	Mandatory	Mandatory role known as Information Officer
Breach reporting deadlines	Within 72 hours	None, but other state laws require 72-hour deadlines	Within a reasonable time period	As soon as reasonably possible
Breach reporting deadlines	4% of global annual revenue or €20 million, depending on which is higher	$7500 per individual violation and personal claims of $750 per incident	2% of a company's Brazilian annual revenue, capped at R$50 million	R10 million fine or 10 years' imprisonment

Table of Contents

Table of Contents

Table of Contents

Table of Contents

GDPR: The EU's Groundbreaking Data Privacy Regulation

GDPR stands for General Data Protection Regulation. It was enacted by the European Union to ensure that profit and non-profit organizations located in Europe and organizations anywhere that process the data of EU residents comply with a strict set of data privacy rules, or else face fines as high as 4% of the company's yearly revenue, capped at €20 million.

Is Your Organization Prepared?

- According to recent studies, the number of completely GDPR-prepared companies is just a mere 20% and only 60% of tech companies

20% of companies are currently GDPR compliant

60% of tech companies have GDPR policies in place

- **Solution**
  Enact policies and employ technology that can align with GDPR best practices, such as NetApp's new Cloud Compliance data mapping technology for the cloud.

Major GDPR Fines

An incomplete list of some of the major fines that have been levied thus far that demonstrate the huge GDPR impact.

$5 Billion

Facebook's Cambridge Analytica Fine
The political research group was able to gain access to the data of 87 million+ Facebook users. The social media giant was then fined a whopping $5 billion in the most significant GDPR accountability action to date and the largest fine that has ever been levied against a US company.

£183,000,000

British Airways
This fine was a result of the data breach at British Airways that exposed the data of half a million users to outside parties. The fine is among the largest levied via GDPR applicability.

£99,000,000

Marriott Hotel
Starwood, a hotel company that had been purchased by the Marriott Hotel, was later discovered to have been undergoing a data breach from 2014-2018. The breach exposed the passwords and credit card information of as many as 30 million GDPR-protected customers.

€50 Million

Google
This fine was levied by the French Data Protection Authority (CNIL) in response to complaints filed by privacy groups who accused Google of violating GDPR guidelines on transparency, unambiguity, and a lack of information in the way that Google accounts were created for the configuration of Android smart phones.

€220,000

Company Fined by Poland's UODO
This anonymously publicized fine was levied against a tech company that scraped the internet for user data, though only attempted to gain consent from a small portion of the users affected. This was the first fine that was levied by Poland's Personal Data Protection Office.

€460,000

Haga Hospital
This fine brought by the Dutch Supervisory Authority for Data Protection (AP) is a response to the hospital's improper handling of patient data, which was discovered when it became known that hospital staff were accessing a celebrity patient's medical file without proper access.

€27,000

Vodafone
The telecommunications giant was fined for receiving a data deletion request from a user; even though the request was acknowledged, the data subject continued to receive texts, meaning that all of the subject's data had not been removed from the company's databases.

1.2M DKK

Taxa 4X35
Taxa 4X35 is a taxi company in Denmark that was found to be retaining data on 9 million of its users, including phone numbers and ride information, in violation of GDPR guidelines on processing personal data.

GDPR: A Breakdown

Territorial Scope

GDPR applies to the data of any resident of the EU that is used by any organization, whether profit or non-profit, that processes that data no matter where that organization is located. This scope effectively extends the GDPR to apply to companies located anywhere in the world, provided that they process the data of EU state citizens and residents.

Definition of Personal Data

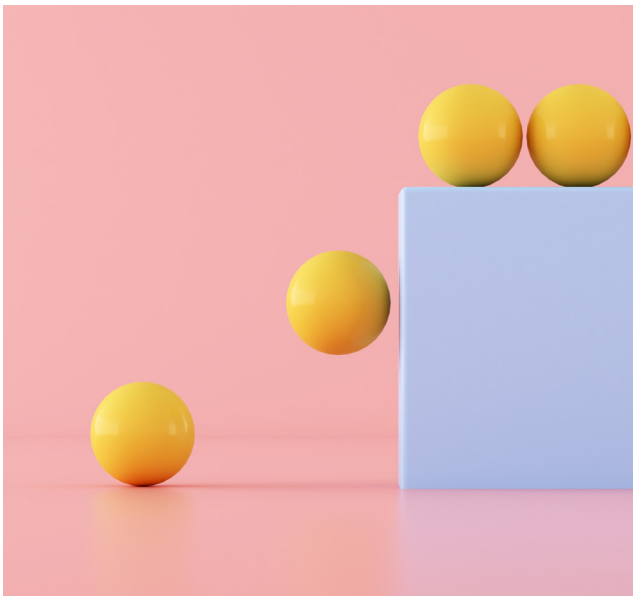
GDPR generally defines personal data as any data that is related to, identifies, describes, or could be associated with a person (or "data subject" as people are referred to in the legislation).

This personal identification can extend to an individual's name, their governmental ID numbers, a customer code created by the company processing the data, online information such as IP addresses or cookies, GPS or other map data, and any reference to a person's biographical information, such as their race, sexuality, philosophical beliefs or religion, economic background, or physical identifiers. Many of these specific traits fall under what GDPR refers to as sensitive personal data, which is information to be afforded the highest levels of data privacy and protection at all times.

Legal Basis for Processing

"Processing" is more or less how GDPR refers to the sale of personal data. Organizations must get consent to collect personal data, with the level of consent varying according to the type of personal data being collected. It is frequent now upon visiting websites to see these kinds of permission screens pop up before being able to access the contents of the website.

The GDPR also looks to limit the amount of data organizations store without any clear purpose. The law stipulates that organizations can only collect personal data that is clearly related to a well-defined business objective. If an organization gathers personal data for one purpose but then decides it wants to use it for other purposes (such as consumer profiling), that could be considered non-compliance.



Data Security

GDPR expects organizations to have some data security precautions in place, but is not specific about what those precautions need to be exactly. The thinking behind this is that data privacy will be achieved via ensuring privacy controls are properly put in place, more so than being able to prevent through specific means breaches from ever taking place. This is because no security measures have ever failed to be completely foolproof from cracked.

Data Transfer

GDPR limits the transfer of personal data from inside the European Economic Area (EEA) to countries outside of it. That effectively makes sure that data privacy can be ensured within the borders of the EU to better protect the data subjects.

There are a few cases where it is possible to transfer data outside of this defined area. Some of these exceptions include making use of what the GDPR calls "appropriate safeguards" which are actually a number of corporate and legislative restrictions, for the purposes of the organization's legal defense, and if the data transfer is being carried out under the terms of a specific contract with the data subject itself.

Rights of Citizens

GDPR has granted EU residents and citizens with a potent number of new data privacy rights. These rights include:

Right to Know

A privacy policy or similar resource must make clear:

- What personal data is collected.
- Why and how the private data is being stored and processed.
- What the legal basis for that data usage is.
- If the data is being shared with 3rd parties and who they are.

Subject Access Request

Companies must create a readable report of all the data on a subject upon request.

Right to be Forgotten

Companies must delete all personal data upon request.

Portability Right

Companies must provide machine-readable copies of all the personal data that they have on a subject upon request.

Right to Accuracy

Companies must use the most up-to-date and accurate personal data available.

Right to be Informed of Breach

Companies have a 72-hour window to inform individuals that their data has been exposed through unauthorized access.

Right to be Informed of Breach

Companies have a 72-hour window to inform individuals that their data has been exposed through unauthorized access.

Partial Opt-Out Right

Individuals can opt-out of specific services.

Right to Oppose Processing

Individuals can refuse to have their data processed, including automated profiling.

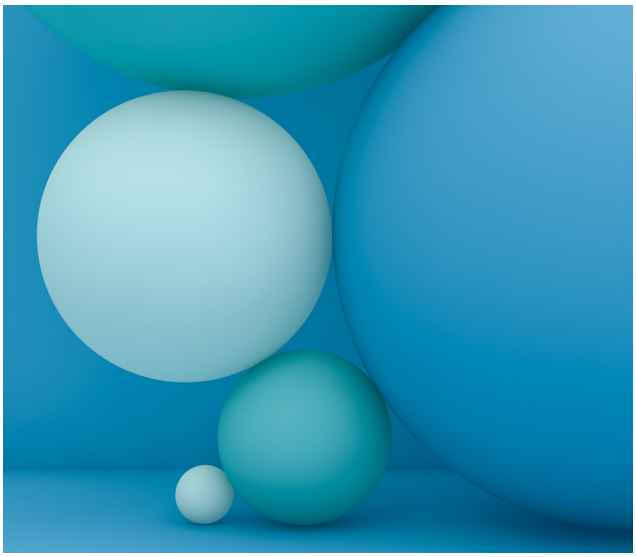
Email Marketing

GDPR has some specific regulations with regards to how email marketing campaigns can be carried out and the data they use. The major factor in this case is that any such campaign can only include a data subject's personal information if that data subject has provided the organization with consent to use their data for such purposes.

That means that data collected and processed automatically through any technological means can't be used to compile email lists and leads without attaining the explicit consent of the data subject first.

Consent Notices and Privacy Policies

As noted above, consent is a major requirement for most of the permissions that organizations have to use the data collected from EU data subjects. Privacy policies must now be clearly and easily accessible according to the GDPR.



Data Protection Officer

GDPR compliance requirements include staffing new positions such as a Data Protection Officer (DPO) and a Chief Privacy Officer (CPO).

Chief Privacy Officer

This c-level position exists at many organizations around the world. Responsibilities include strategizing and ensuring the company's overall privacy stance.

Data Protection Officer

A role that is mandated by GDPR Article 39. According to GDPR, this individual must operate on a more independent level within the organization, acting essentially a self-policing officer.

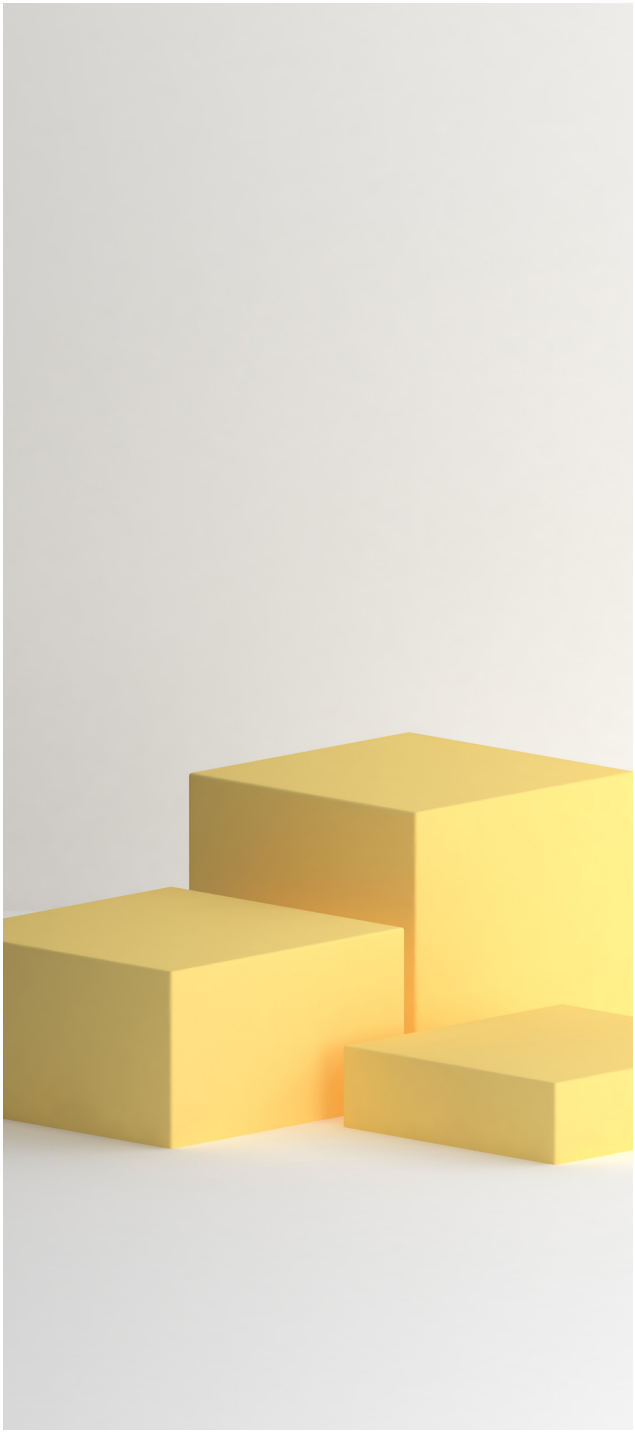
Reporting a Data Breach

Data breaches can potentially expose personal data and sensitive information that belongs to EU data subjects protected by GDPR.

The regulation gives companies that have become aware of a data breach 72 hours to notify all affected and potentially affected data subjects of the event.

Financial Penalties

One of the most unique aspects of the GDPR is its "teeth"—very stiff penalties for non-compliance (up to €10 million or 2% of worldwide annual turnover, whichever is higher) and breaches (up to €20 million or 4% of worldwide annual turnover, whichever is higher). Just as painful is the right of Data Protection Authorities to prevent a company from collecting or processing personal data while a suspected non-compliance or breach is being investigated.



Affecting Companies Located In or with Data Subjects In:

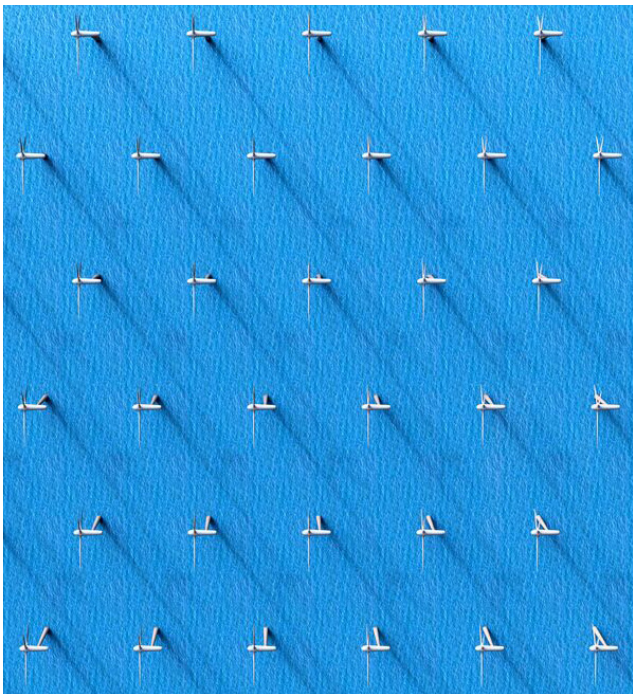
- Austria
- Belgium
- Bulgaria
- Croatia
- Republic of Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden

Growing Global Awareness

New Privacy laws similar to GDPR have been enacted around the world:

- The California Consumer Privacy Act (CCPA) in California (US)
- The Protection of Personal Information Act (POPI) in South Africa
- The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada
- LGPD, the General Data Protection Act in Brazil
- The Data Protection Act of 2018 in the United Kingdom.
- Various privacy laws in effect in Australia.

In the following sections we'll take a look at a number of these newer data privacy laws and see how they compare to GDPR.



CCPA: A Data Privacy Model for the US

On January 1, 2020, a new data privacy law came into effect in California, the largest state in the US. It's wide-ranging data privacy regulations are largely modelled on those of the EU's GDPR, though with some major differences. It's reach affects certain organizations that collect and use personal data about citizens of California. The California Consumer Privacy Act (CCPA) is designed to give residents of the state more control over their personal data and requires companies to become more transparent about the data they collect and store about consumers.

What is most significant about this regulation, aside from its very clear imperative for businesses to respect data privacy, is that it is likely the forerunner of other legislation to be enacted in the United States, both on at the state and federal level. That makes the differences between how CCPA works versus how GDPR works quite important to understand.

CCPA Introduction

The California Consumer Privacy Act (CCPA) is a data protection law that the State of California enacted in response to growing public concern over the abuse of personal data. CCPA gives California residents more visibility and control over the information that websites and applications collect about them.

When you consider how many consumers could be affected, that could potentially mean huge fines for companies large and small.

The CCPA complements existing state privacy regulations, such as the California Online Privacy Protection Act (CalOPPA), but it also introduces new requirements in the following key areas:

When the California Consumer Privacy Act (CCPA) came into effect on 1 January, enterprises were forced to think again about the way they protect personal data in the wake of more new data privacy legislation.

They've been presented with new IT challenges where, just as regulations have been tightening up, they've been storing information on an increasingly diverse range of storage systems and data formats.

Not all solutions are up to the job or geared towards the modern cloud landscape, where companies store data in a huge variety of structured and unstructured forms. As a result, CCPA compliance calls for a new breed of data protection tooling—with features that can perform the following functions.

Who it covers

California residents ("Consumers") whether or not they are US citizens.

- A California resident is defined as someone who is subject to California taxation.

CCPA vs. GDPR

What are the major differences between these two laws and how are they going to affect your company? For the most part, GDPR is far wider in scope.

For example, by contrast with GDPR, you don't need to obtain prior consent for simply collecting and processing personal data according to CCPA. But just because you're compliant with GDPR doesn't necessarily mean you comply with CCPA. Although GDPR and CCPA share many common features, you'll still need to meet specific requirements in relation to the sale of personal data.

This section aims to give you an easy resource to parse the differences between these two game-changing data privacy regulations.

Territorial Scope

The CCPA applies to any for-profit concern that does business in California, collects personal data about California residents, and meets one or more of the following thresholds:

- It brings in annual gross revenues of at least US$25 million.
- It collects personal information from 50,000 or more Californian residents, households or devices per year.
- It generates more than 50% of its annual revenue by selling personal information about California residents.

Although the CCPA doesn't define what doing business in California means, you're likely to come under the definition if your business:

- Is based in California.
- Has employees in California.
- Has connections with California through ownership of real estate or repeated sales to customers in the state.

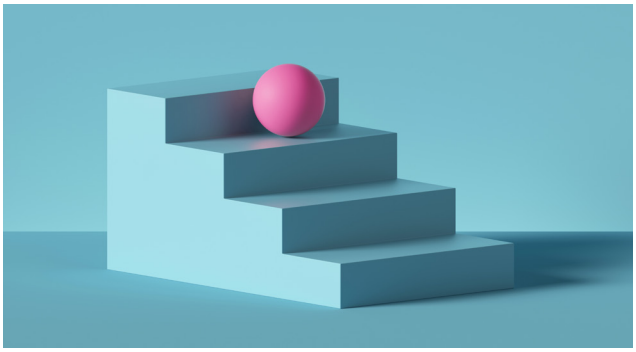
Definition of Personal Data

CCPA applies to personal data:

- Provided directly by users in online forms
- Collected by tracking tools and related technologies

This information includes anything that can be used to identify, describe, or be associated in any way with a particular California resident or "household." The emphasis on household is because this is a curious term for CCPA to use as it is undefined in the document.

CCPA differs from GDPR in that it has no specific restrictions placed on sensitive personal information about individuals, though it does include provisions that prevent personal data from being used to discriminate against an individual (see below).



Legal Basis for Processing

CCPA gives businesses the opportunity to process or sell personal data of California residents, given that those residents were offered a clearly stated the option to opt out of such transactions. What CCPA considers the sale of data is quite expansive however, as it is not specifically restricted to a financial exchange. Data can be considered sold from one company to another if it was done for some other "valuable consideration."

Whereas GDPR gives data subjects the right to prevent companies from using their personal data for marketing purposes, CCPA opt-out rights are more concerned with the sale of personal data.

Data Security

Similar to GDPR, CCPA doesn't have a specific requirement when it comes to data security, though it does leave the door open for private action taking place should a data breach take place and allege that the business did not take reasonable steps at the security level to prevent such an event from occurring.

Data Transfer

CCPA does not limit the transfer of data outside of the US. GDPR has strict rules about how data can be transferred, and generally it is not possible to do so outside of the EEA. As a country with state-by-state data privacy laws, the US doesn't currently provide such protection. So, currently, the European Commission will only allow transfers that are covered by the EU-US Privacy Shield framework.

Rights of Citizens

The CCPA has granted new privacy rights to California citizens, who can now request the personal data you store about them. You must provide this information promptly and, under normal circumstances, within **45 days**. In addition, California residents can also request you delete their data.
In the case of either of the two rights, you can only decline a request under certain conditions and must administer requests free of charge. It's therefore essential you're able to remove or retrieve information about a customer as quickly and efficiently as possible. But, without the right tooling, this can be a complex and protracted process involving a multitude of business departments and extensive manual labor.

Other rights include

Right to Opt-Out

Consumers can choose for their data not to be shared with or sold to outside parties.

Right to Delete

Companies must delete all of the data held on a Consumer upon request, with certain legal exceptions.

Right to Non-Discrimination

The company is not allowed to change a Consumer's service levels or prices due to the Consumer invoking rights outlined by CCPA.

Email Marketing

Where there is a specific focus on email marketing in the GDPR, CCPA does not have any provisions that specifically pertain to email marketing.

Consent Notices and Privacy Policies

With CCPA in effect, companies will now only be able to sell personal data about California residents under the age of 17 if they've given you prior consent to do so.

Those aged 13–16 will be able to authorize the sale of their data themselves. However, in the case of children under the age of 13, it is required to obtain consent from a parent or guardian.

Data Protection Officer

Unlike the GDPR, CCPA does not require the appointment of a dedicated data protection officer, or any similar role (including a chief privacy officer, or CPO).

Reporting a Data Breach

The CCPA doesn't have specific data breach deadline requirements. There is also another law, the California Data Breach Notification Law, that CCPA acts in accordance with. Note that there are certain circumstances where data that is breached would be actionable according to the notification law but NOT under CCPA.

Financial Penalties

The Californian state can impose a civil penalty of up to **$7,500 per violation** on any company that is in breach of the CCPA and fails to address the requirements of the law within **30 days**. In addition, any California citizen will also have the right to pursue damages of up to **$750 per incident** in the event of exposure. So not meeting CCPA compliance goals can be costly.

CCPA Fines

$7,500 per violation if non-compliant within **30 days**.

$750 per incident can be sued by private individuals when data is exposed.

LGPD: Brazil's Version of the GDPR

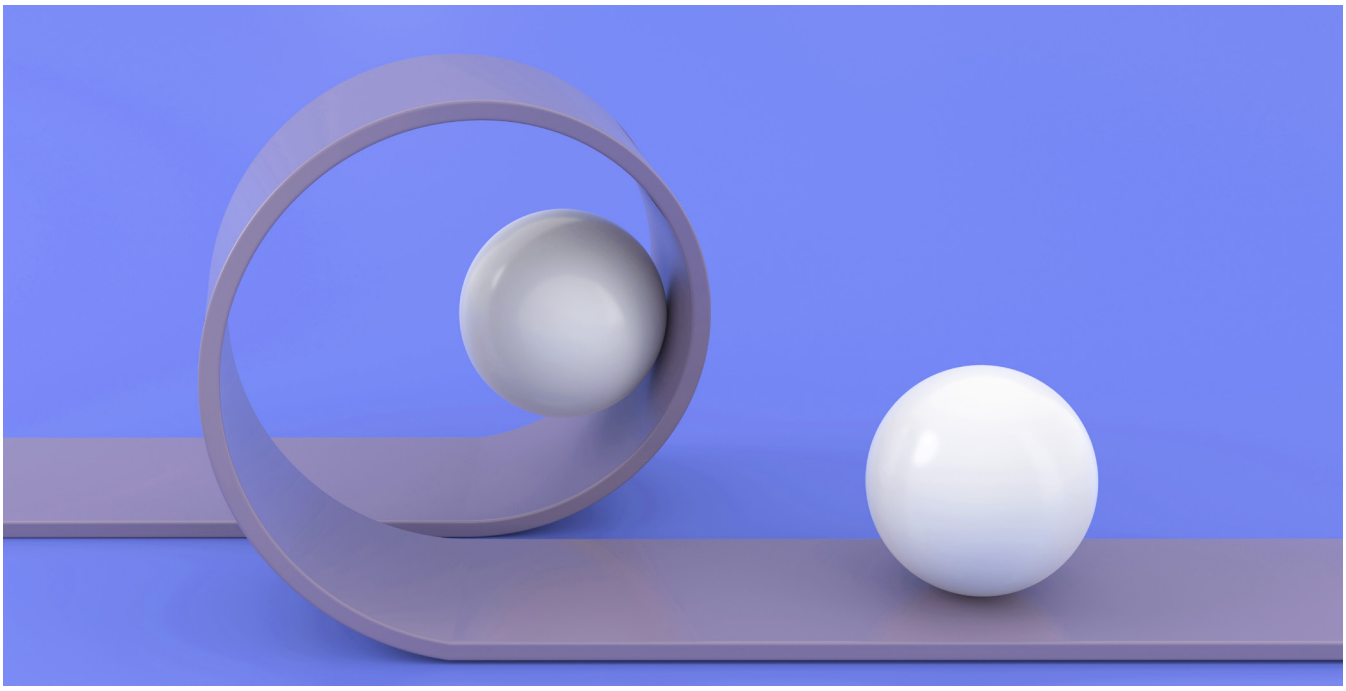
Storage, compliance, and security teams across the world are reviewing their data protection practices in response to the forthcoming **Lei Geral de Proteção de Dados Pessoais (LGPD)**, a Brazilian data privacy law similar to the General Data Protection Regulation (GDPR).

The LGPD will be the latest in a string of tighter data protection laws aimed at addressing public concern about the widespread use of their data. The new law has been long in the making.

After a lengthy delay, it was finally due to come into force in August this year. But, owing to the impact of the coronavirus pandemic, the Brazilian government has pushed back the effective date yet again to give organizations more time to prepare for the legislation.

But with many enterprises still struggling to comply with other new data privacy regulations, the delay of LGPD is giving companies an opportunity to start making plans to meet LGPD requirements as soon as possible. In some cases, provisions will be identical to those put in place to meet GDPR's standards. But in other cases there will be subtle differences.

In this post, we run through the key features of the long-awaited LGPD, Brazil's approach to such legislation, and how it compares with its European counterpart.



The LGPD in a Nutshell

With LGPD, Brazil sets out to harmonize a multitude of disparate statutes into a unified set of standards. It strengthens the data privacy rights of Brazilian nationals through tighter controls over how companies are allowed to store and process personal data.

It is also designed to promote privacy best practices and help enterprises leverage compliance as an opportunity to drive more revenue. Moreover, it frees up competition by allowing private companies to process personal data for use by the public sector.
Though less extensive than the European regulations, the LGPD aims to achieve much the same privacy objectives. As a result, the two laws are remarkably similar, sharing a common focus on **accountability, security, data minimization, purpose limitation, and privacy by design.**

LGPD vs. GDPR: A Comparison

Territorial Scope

In relation to the territorial scope of each law, the LGPD and GDPR follow the same basic principle. Namely, they apply to any organization that stores or processes personal data about the citizens in the territorial jurisdiction they cover—regardless of where they're located in the world.

In other words, wherever you're based, if your business offers goods and services to the Brazilian market, you'll need to take steps to comply with the LGPD.

Definition of Personal Data

Whereas the GDPR is very specific about what constitutes personal data, under the LGPD it is far less clearly defined. However, this may change in the future as the law comes into everyday use.

On the other hand, the LGPD mirrors the GDPR by designating certain types of information, such as that concerning an individual's racial or ethnic origin, health or trade union membership, as sensitive personal data, where special rules apply.

Legal Basis for Processing

As with the GDPR, the LGPD sets out a list of lawful grounds for processing personal data. These are broadly similar, such as to meet a legal or contractual obligation or where the individual has given consent for you to process their personal data for a specific purpose.

However, with LGPD, Brazil does explicitly allow a legal basis for personal data use which isn't directly covered by the GDPR: processing someone's personal data for the purpose of protecting their credit score. Nevertheless, in most cases, the GDPR would still interpret this as an appropriate basis for processing—on the grounds that it is in the legitimate interests of the consumer.

Data Security

For both Europe and Brazil, data privacy law entails data security. Under both the LGPD and GDPR, you are required to implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, alteration, or destruction.

The Brazilian body responsible for enforcing data protection, the National Data Protection Authority (ANPD), is tasked with providing more detailed guidance to the minimum technical standards you'll be required to adopt.

The GDPR doesn't directly specify the security measures you should have in place. However, national enforcement agencies, such as the Information Commissioner's Office (ICO) in the UK, each offer a broad guide to meeting your security obligations.

Data Transfer

The LGPD takes the same line as the GDPR by prohibiting the transfer of personal data out of Brazilian territory, except in certain circumstances or to countries that provide a strong regulatory level of data protection.

This could have data residency implications for companies based in the US, which currently follows a patchwork approach of state-by-state data protection regulations rather than a unified nationwide legal framework.

Rights of Citizens

Both laws essentially grant data subjects the same basic rights. For example:

Consent: You're only able to process and store data about a Brazilian individual with their consent, which they can revoke at any time.

Data Subject Access Requests (DSARs): The LGPD grants Brazilians the same fundamental rights of access, including right to correction and right to erasure, as the GDPR does for EU citizens.

However, under the LGPD, you must respond to a DSAR within 15 days. This may mean you'll need to improve your DSAR response procedures, as it is a significantly shorter period than the one month allowed by the GDPR. Meeting that kind of tight deadline will largely depend on your ability to automate your DSAR reporting.

Email Marketing

Whereas the GDPR applies strict rules to email marketing and text messaging, it is an area not directly covered by the LGPD.

However, as with the GDPR, it still makes sense to seek an individual's approval to receive marketing emails and text messages, as this activity is likely to constitute a form of data processing that requires consent.

Consent Notices and Privacy Policies

The LGPD approach to obtaining consent is very much the same as that for the GDPR. According to LGPD, a customer's consent must be specific, informed, unambiguous, and freely given. In other words, you should be upfront about what exactly an individual is consenting to and give them proactive control over how you use their data.

You should reflect these requirements in the design of your signup forms, online checkouts and cookie consent notices. Although the LGPD makes no direct reference to privacy policies, you should still revisit your policy wording to ensure it meets transparency obligations.

In addition, consent should be granular, with separate consent for different processing activities. What's more, you should maintain records of valid consent. And data subjects should also be able to easily revoke consent at any time.

Data Protection Officer

To comply with the GDPR, you *may* need to appoint a data protection officer (DPO). However, this only applies to public-sector organizations and private companies that store and process personal data at scale.

By contrast, as things stand under the LGPD, you must appoint a DPO, as it applies to any organization that processes the personal data of Brazilian citizens. However, in practice, this is likely to prove problematic and will inevitably require clarification by the Brazilian enforcement authorities.

The duties of DPO don't necessarily have to be performed by an individual. They may be carried out by an internal team or outsourced to a third-party, such as a specialist DPO service. Note also that the DPO role is separate and unique from that of the chief privacy officer, or CPO.

Reporting a Data Breach

In the event of a breach that could potentially infringe the privacy rights of data subjects, under both the LGPD and GDPR, you must notify both the relevant data protection authority (DPA) and the individuals affected.

The LGPD only states you must do this within a reasonable time period, as defined by the ANPD. The GDPR is more specific, giving you just **72 hours** to notify the DPA after you are aware of a breach.

Financial Penalties

Monetary penalties for breaking LGPD rules are relatively modest compared with the GDPR. The maximum fine for a violation is **2%** of a company's Brazilian annual revenue and is capped at **R$50 million** (about €7.84 million or $9.28 million) per offense.

This compares with GDPR fines of up to **4%** of global annual revenue or **€20 million**, whichever is the higher.

POPIA: South Africa's Version of the GDPR

On 1 July 2020, South Africa's Protection of Personal Information Act (POPIA) finally came into force, coming hot on the heels of other new privacy regulations, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

Most sections of the act are now officially law. But compliance isn't mandatory until the remaining part of the legislation, which grants enforcement powers to South Africa's new regulatory authority the Information Regulator, comes into effect on **1 July 2021**.

This means that, if your organization is subject to the POPIA, you only have a few months to comply.

In this post, we give you a brief introduction to the new legislation and help you decide whether your company comes within the scope of the law. We'll also guide you through the main differences and similarities between the POPIA and its European counterpart, the GDPR.

POPIA in a Nutshell

The POPIA is the latest in a succession of new data protection laws aimed at strengthening the privacy rights of individuals in today's data-driven landscape.

The law was ratified in November 2013—several months before the EU voted to adopt the GDPR. But progress subsequently stalled for several years until the South African government finally gave it the green light in 2020.

POPIA vs. GDPR

Despite its slightly earlier origin, the POPIA is still very similar to the GDPR, sharing much the same guiding principles, including **accountability**, **transparency**, **security**, **data minimization**, **purpose limitation** and the **rights of data subjects**.

Territorial Scope

In general, unless your organization is based in South Africa, it's unlikely you'll need to comply. But if you're a large-scale enterprise the answer isn't quite so simple.

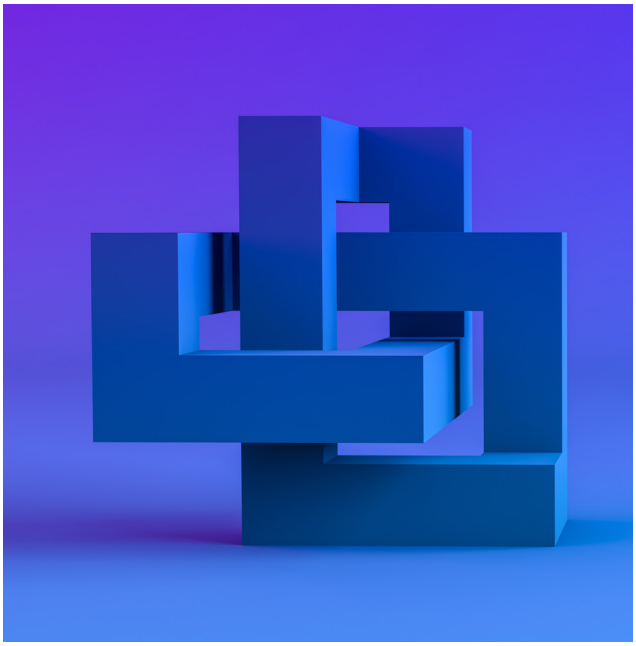
This is because the scope of the POPIA is different from other new data protection laws, where what matters is the location of processing rather than the location of the data subject.

For example, the GDPR applies to any organization that processes personal information about European Economic Area (EEA) citizens regardless of where it's based in the world.

However, the POPIA only applies to companies based in South Africa or those that process personal data within South African borders. So, to check whether you need to comply, you'll need to find out exactly where you're processing personal data.

This should include the whereabouts of not only your on-premises data centers but also your cloud-based deployments.

Your cloud infrastructure will likely be the deciding factor, as both AWS and Microsoft Azure now have cloud regions in South Africa. So your company could well be using them in a bid to bring your data closer to African customers.



Definition of Personal Data

In terms of how it defines personal data, the POPIA is more extensive than the GDPR, as it covers not only the information you collect about individuals but also about companies and other types of organization.

This is a significant departure from other data privacy laws. So it's not yet clear how exactly it'll work in practice. However, as your first step to compliance, you should reflect the new legal requirements in your contracts with partners, suppliers and vendors.

As with the GDPR, the POPIA classifies a separate subcategory of personal data, known as **special personal information**, which is more sensitive and therefore subject to stricter requirements. This mainly relates to an individual's:

- religious or philosophical beliefs,
- race or ethnic origin
- trade union membership
- political persuasion
- health
- sex life or sexual orientation
- physical, physiological or behavioral characteristics (biometric data)

In addition, the POPIA applies to the personal data of any individual—regardless of their nationality. So while the GDPR is only designed to protect EU citizens, the POPIA protects anyone whose personal data is processed within South African territory or by a South African undertaking.

Consent and Privacy Policies

Unlike the GDPR, you don't generally need to seek consent to collect an individual's personal information. However, you must still do so where you collect any type of special personal information.

Specific consent rules also apply to collection of data about **children**, aged 17 and under, where you normally need the consent of a competent person, such as a parent or guardian.

In addition, you may only process personal data for **direct marketing** (by email, telephone or SMS) where the data subject is a customer or has given their consent to processing.

However, you must give customers a reasonable opportunity to object to processing if they wish. And, as with the GDPR, your communications should include details on how to opt out of your marketing list.

Similar rules to the GDPR also apply regarding transparency. This basically means that, wherever you collect personal data about individuals, you must be upfront about:

- who you are
- what information you collect
- why you collect it
- the rights of data subjects

As with the GDPR, the most practical way of providing this information is to incorporate it into your online privacy policy.

Legal Basis for Processing

Even though you don't necessarily need consent to collect personal data, you must still meet all other POPIA conditions for lawful processing.

These share much in common with other new data protection laws, such as similar requirements for data security, data transfer and rights of access.

However, you'll need to be aware of one distinctly different condition where, in all but a few certain circumstances, you may only collect data directly from the data subject.

Data Security

Both the POPIA and GDPR outline only very general data security requirements by merely stating you must implement **appropriate technical** and **organizational measures** to protect personal data in your possession.

This basically allows you to tailor security measures to the nature of the personal data you process, impact level of a potential breach and cost of implementation.

Neither law really goes into any further detail—although the POPIA does mention you should give due regard to generally accepted security practices and procedures.

Data Transfer

In general, the POPIA and GDPR prohibit transfers of personal data outside of South Africa and the EEA respectively.

However, in the case of the POPIA, cross-border transfers are permitted to a third party that is subject to legal or corporate data protection rules substantially similar to its own.

The GDPR works on similar lines, where international transfers are only permitted to specific countries with legal frameworks that provide adequate protection of personal data.

Under both laws, certain types of transfer are exempt from the conditions, such as when an individual has consented to the transfer or where the transfer is necessary to fulfill a contract.

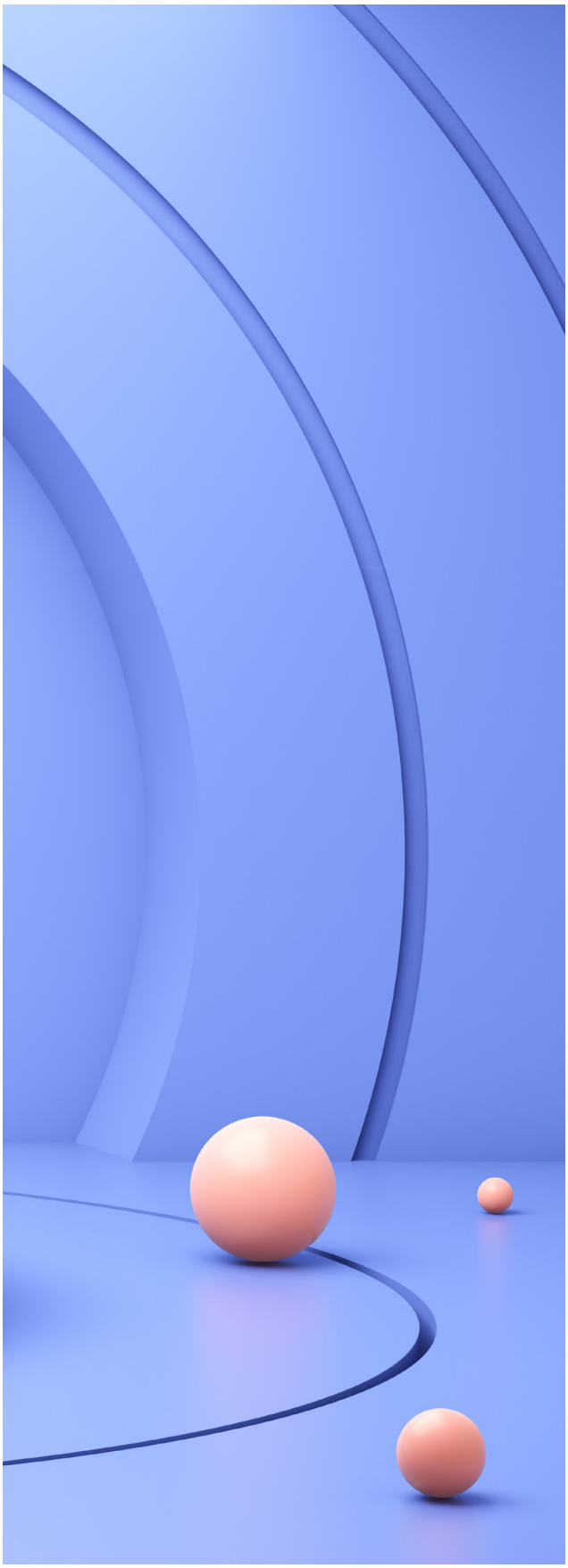
Right of Access

The POPIA grants data subjects similar rights of access, correction and erasure as the GDPR.

Under both laws, citizens may request, free of charge, confirmation of whether or not you process their personal information.

But, unlike the GDPR, the POPIA allows you to charge a fee for providing individuals with a copy of the information you hold about them. If you choose to do so, you must give a written estimate of the cost before you provide the service.

The POPIA only states that you must respond to any such request within a reasonable time. The GDPR, on the other hand, is more specific—where, under normal circumstances, you must respond to a **data subject access request (DSAR)** without delay and within **a month** at the latest.



Information Officer

The POPIA designates the role of information officer with similar responsibilities to those of a data protection officer (DPO) under the GDPR.

But, whereas a DPO is only mandatory for public sector bodies and private companies that process data at scale, all organizations that come within the scope of the POPIA must appoint an information officer.

In the absence of a formal appointment, the role of information officer falls to the head of your organization—usually the chief executive officer (CEO).

Breach Reporting

The POPIA procedure for reporting a data breach is very much like that of the GDPR—where, in general, you must notify both the relevant regulatory body and the individuals affected by the compromise.

The POPIA simply states you must do this as soon as reasonably possible after becoming aware of the breach. However, the GDPR specifically requires you to notify your supervisory authority within **72 hours**.

Penalties for Non-Compliance

At R10 million, the maximum financial penalty for a POPIA infringement is significantly lower than a potential GDPR fine, which can reach up to **€20 million** or **4% of annual global turnover**.

However, under South African legislation, individuals can be held criminally responsible and sentenced to **prison for up to 10 years** in more serious cases.

What's more, POPIA sanctions not only apply to non-compliance but also a range of other offenses, which include:

- hindering, obstructing or unlawfully influencing enforcement officials
- failing to attend court hearings
- lying under oath

By contrast, GDPR sanctions focus more directly on non-compliance. Nevertheless, when setting a fine, European enforcement authorities may still consider the degree of cooperation an organization shows during their investigations.

Conclusion: Towards a Data Privacy Without Borders

While data is growing at a faster rate, the ability for data privacy regulations to control that data is helping to shrink the world a little bit. The first steps taken by the EU with the enactment of GDPR have started to be seen around the world.

California, as the largest state in the US has enacted a law that, while lesser in scope than GDPR, still establishes clear guidelines on the appropriate use of personal data. It's a model that may soon be replicated throughout the country, possibly on a national level. In a country as large and economically vibrant as Brazil, data protection law was an inevitability. Virtually any company with a global presence will process personal data about Brazilian consumers. The need to comply with the LGPD will soon be a worldwide requirement. South Africa in its approach to data protection is focused more nationally; though as an economic and cultural hub POPIA's restrictions will affect many international businesses. Because so many of these regulations have similar stipulations, a general guideline to have data privacy by default as the starting point in your business will help handle these and the data privacy regulations to come.

To help meet your privacy requirements anywhere in the world, try NetApp Cloud Compliance.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NA-000-1020